

I CLAIM:

1. A method for securely transmitting streamed media consisting of a stream header and a series of data packets between a sender and a recipient comprising the steps of:

generating a random base key,
encrypting said base key to create an open key,
transmitting said open key to said recipient,
encrypting each packet of the data in the stream by:

(a) assigning a tag value to each packet if no tag value already exists,
(b) creating a packet key by computing a secure hash of said base key and the tag value or the assigned tag value of the packet,

(c) encrypting the data in the packet using said packet key, and
(d) adding said tag value to the corresponding encrypted packet data and

inserting the packet so processed into the packet stream,
transmitting the encrypted packet stream to said recipient,

at the recipient's station receiving said open key and the encrypted packet stream,
decrypting said open key to derive the base key,

decrypting each received encrypted packet in the stream by:

(a) extracting the tag value from each packet,
(b) recreating said packet key by computing a secure hash of the base key and the packet's tag value,

(c) decrypting the packet data using said packet key,
(d) and storing or outputting the decrypted packet data in a form suitable for playing the streamed media.

2. A method according to claim 1 wherein said open key is transmitted to the recipient by adding it to the stream header and then extracted from the stream header at the recipient's station for decryption.

3. A method according to claim 1 wherein said base key is encrypted using a public key encryption algorithm in conjunction with the recipient's public key and wherein said open key is decrypted using said public key encryption algorithm in conjunction with the recipient's private key.

4. A method according to claim 1 wherein said packet data is encrypted using a symmetric encryption algorithm in conjunction with said packet key and said encrypted data is decrypted at the recipient's station using said symmetric encryption algorithm in conjunction with said recreated packet key.

5. A method according to claim 1 wherein the hash function used to create and re-establish said packet key is SHA-1 or MD5.

6. A method for securely transmitting streamed media consisting of a stream header and a series of data packets between a sender having the recipient's public key and a recipient having a private key, comprising the steps of:

generating a random base key,

asymmetrically encrypting said base key using the recipient's public key to create an open key,

transmitting said open key to said recipient,

encrypting each packet of the data in the stream by:

(a) assigning a tag value to each packet if no tag value already exists,

(b) creating a packet key by computing a secure hash of said base key and the tag value or the assigned tag value of the packet,

(c) encrypting the data in the packet using said packet key and a symmetric encryption algorithm, and

(d) adding said tag value to the corresponding encrypted packet data and inserting the packet so processed into the packet stream,

transmitting the encrypted packet stream to said recipient,

at the recipient's station receiving said open key and the encrypted packet stream,

decrypting said open key using the recipient's private key to derive the base key,
decrypting each received encrypted packet in the stream by:

- (a) extracting the tag value from each packet,
- (b) recreating said packet key by computing a secure hash of the base key
5 and the packet's tag value,
- (c) decrypting the packet data using said packet key and said symmetric
encryption algorithm,
- (d) and storing or outputting the decrypted packet data in a form suitable for
playing the streamed media.

10

7. A method according to claim 6 wherein said open key is transmitted to the
recipient by adding it to the stream header and then extracted from the stream header
at the recipient's station for decryption.

15

8. A method according to claim 6 wherein the hash function used to create and re-
establish said packet key is SHA-1 or MD5.